Date of acceptance : 23/01/2015

WRITTEN OBSERVATIONS OF THE ITALIAN REPUBLIC

Case C-362/14 *

Document lodged by:

Italian Government

Usual name of the case:

Schrems

Date lodged: 6 November 2014

* Language of the case: English.

33283/ - 398 Case C-362/14

AVVOCATURA GENERALE DELLO STATO

THE COURT OF JUSTICE OF THE EUROPEAN UNION

OBSERVATIONS

Of the Italian Republic acting through the Agent appointed for these proceedings, Gabriella Palmieri, represented and defended by the Avvocatura generale dello Stato (State Legal Advisory Service) by that Avvocato dello Stato (State Legal Representative) with an address for service at the Embassy of Italy to Luxembourg;

In the reference for a preliminary ruling, *Schrems* C-362/14, made by order of 25 July 2014 by the High Court of Ireland.

*****

1 By its order for reference mentioned above, the High Court of Ireland asks the Court of Justice to give a ruling on the following question: 'Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?

Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?'

2 In that regard, the Italian Government notes that Article 25(6) of the Directive 95/46 provides '*6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.*

Member States shall take the measures necessary to comply with the Commission's decision.'

3 Such a provision cannot be read separately from Article 28(3), which provides '*3. Each authority shall in particular be endowed with:*

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.'

4 The effect of the adoption by the Commission of a decision within the meaning of Article 25(6) is that the data processing regime in force in a third country is considered to be equivalent to the regime in force in the European Union and to be consistent with the Directive. That effect cannot, however, lead to a reduction of the protection afforded to the parties concerned by the data processing, who are resident within the European Union, concerning the data transferred to a third country subject to a decision under Article 25(6), compared to the level of protection that those parties would enjoy were their data processed in the European Union.

5 The powers of supervision, protection and punishment invested in the data protection authorities under Article 28(3) undoubtedly form part of that level of protection. There is, therefore, no reason to believe that those authorities may not exercise those powers also over transfer of data to third countries which are the subject of a decision under Article 25(6). Otherwise, the protection afforded to Union citizens in respect of that latter data would be lower than the protection over the data processed within the Union. The effect of the adoption of a decision under Article 25(6), ultimately, is limited to removing the general prohibition of the transfer of personal data to third countries which fail to ensure a standard of protection comparable to that offered under the Directive. It is certainly not to create a special regime for the transfer to third countries of data which is the subject of that decision,

which is different and 'privileged' (to the detriment of European citizens) as compared to the general regime provided for by the Directive for data processed within the European Union.

6 It must, in any event, be recognised that even the decision under Article 25(6) in question in the present case supports that conclusion, given that it is stated in Article 3(1)(b) that the Member States' data protection authorities may exercise their powers in cases where there is a substantial likelihood that the principles referred to in the FAQs are being violated or there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue.

7 Therefore, specifically in respect of the issue raised in the order for reference, which is that, in the United States, the personal data transferred would be subject to indiscriminate access and use by the police and judicial authorities for the purpose of safeguarding national security, it must be recalled that the Court of Justice has recently made it clear (in its judgment of 8 April 2014, C-293/12 and C-594/12, paragraphs 51 *et seq.*) that

> 51 As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.
>
> 52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C‑473/12 *IPI* EU:C:2013:715, paragraph 39 and the case-law cited).
>
> 53 In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.
>
> 54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and S. and *Marper v. the United Kingdom*, § 99).
>
> 55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent

on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

8 That restrictive interpretation of the guarantees granted to European citizens by Articles 7 and 8 of the Charter must also be valid when Directive 95/46/EC, at issue in this case, is applied. The directive could not, therefore, in any event be interpreted as meaning that the decision under Article 25(6) could have the effect of depriving European citizens of the guarantees afforded under those articles of the Charter, whenever it is found that such guarantees do not exist in substance in the third country to which personal data is transferred.

*****

Accordingly, the Italian Republic claims that the Court of Justice should, in response to the request for a preliminary ruling, rule that Article 25(6) of Directive 95/46/EC must be interpreted as not precluding national personal

data protection authorities from exercising, in the case of the processing of the data transferred to a third country subject to a decision taken under that article, all the powers of protection granted to them by, in particular, Article 28 (3) of the Directive; and that, in any event, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union prohibit, even where the decision is taken pursuant to Article 25(6) of the Directive, personal data from being transferred to the third country to which it relates where those data are accessible indiscriminately by the judicial authorities and police of that state, even if those judicial authorities and police rely on considerations of national security.

Rome, 6 November 2014

Paolo Gentili

avvocato dello Stato